APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/591,385	05/31/2007	Michael J. Wynne	G40.2-13340	1895

490   7590   09/08/2008
VIDAS, ARRETT & STEINKRAUS, P.A.
SUITE 400, 6640 SHADY OAK ROAD
EDEN PRAIRIE, MN 55344

EXAMINER
WRIGHT, BRYAN F

ART UNIT	PAPER NUMBER
2131	

MAIL DATE	DELIVERY MODE
09/08/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

	Application No.	Applicant(s)
Office Action Summary	10/591,385	WYNNE ET AL.
	Examiner	Art Unit	
	BRYAN WRIGHT	2131	

-- *The MAILING DATE of this communication appears on the cover sheet with the correspondence address* --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE <u>3</u> MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1) ☒ Responsive to communication(s) filed on *31 May 2007*.
2a) ☐ This action is **FINAL**.   2b) ☒ This action is non-final.
3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4) ☒ Claim(s) *1-22* is/are pending in the application.
    4a) Of the above claim(s) _____ is/are withdrawn from consideration.
5) ☐ Claim(s) _____ is/are allowed.
6) ☒ Claim(s) *1-22* is/are rejected.
7) ☐ Claim(s) _____ is/are objected to.
8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9) ☐ The specification is objected to by the Examiner.
10) ☒ The drawing(s) filed on *31 August 2006* is/are: a) ☒ accepted or b) ☐ objected to by the Examiner.
    Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
    Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12) ☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
    a) ☒ All   b) ☐ Some * c) ☐ None of:
       1. ☒ Certified copies of the priority documents have been received.
       2. ☐ Certified copies of the priority documents have been received in Application No. _____.
       3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).
    * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date *10/10/2006*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1.   This action is in response to application filed on May 31, 2007. Claims (1-

22) are pending.

Priority

2.   Applicant's claim for benefit of foreign priority under 35 U.S.C. 119 (a) - (d)

is acknowledged.

The application is filed on May 31, 2007 but is a 371 case of

PCT/AU05/00317 application filed 03/04/2005 and has a foreign priority

application Australia 2004901143 filed on 03/05/2004.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35

U.S.C. 102 that form the basis for the rejections under this section made in this

Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

3.   Claims 1-22 are rejected under 35 U.S.C. 102(b) as being anticipated by

Graham et al (US Patent Publication No. 2002/0178271 and Graham

hereinafter).

4.   As to claim 1, Graham teaches a **access control system for controlling**

access to data stored on at least one data storage medium of a computing

system, the access control system comprising:

authentication means to authenticate users permitted to access data

stored in the at least one data storage medium (i.e., ... teaches a n end-user

client device requests a file from the content source 160, the request is received

by the proxy system, which selectively provides the requested file as a function of

information the proxy system obtains from authentication system and policy

system [par. 65]]);

and database means arranged to store data access profiles (i.e., 360,

fig. 3);

each data access profile being associated with a user permitted to

access data stored in the at least one data storage medium (i.e., ... 510, fig.

5).

each data access profile including information indicative of the

degree of access permitted by a user to data stored in the at least one data

storage medium (i.e., ... teaches the proxy system 110 determines if the

requesting user has the right to access the file [par. 66]);

and each data access profile including a master data access profile

and a current data access profile, the current data access profile being

modifiable within parameters defined by the master data access profile (i.e.,

...teaches all content access policies are maintained via the policy editor. ... this

his service performs internal policy consistency validation, rights revocation, and synchronized policy updates [par. 111]).

5.   As to claim 2, Graham teaches a **access control system further comprising profile setting means arranged to facilitate creation of the master and current access profiles** (i.e., … teaches the authentication service creates credentials used to gain access to the protected content [par. 105]).

6.   As to claim 3, Graham teaches a **access control system where the access control system is incorporated into a computing system having an operating system and the master data access profile is modifiable only prior to loading of the operating system** (i.e., … teaches a service performs internal policy consistency validation, rights revocation, and synchronized policy updates [par. 111] Those skilled in the art would recognize inherent to the capability to synchronize policy (i.e., .. **access profiles**) updates is the ability schedule modification of policies) … further teaches at the time that the DCMS server application is booted, a specified file path is checked. If there are Plug-Ins available, then the DCMS server application loads these plug-ins, and continues booting [par. 371])

7.   As to claim 4, Graham teaches a **access control system where said control system is activatable so as to permit modification of the current access profile and deactivatable so as to prevent modification of the**

current access profile (i.e., ... teaches a service performs internal policy

consistency validation, rights revocation, and synchronized policy updates [par.

111] Those skilled in the art would recognize inherent to the capability to

synchronize policy updates is the ability to activate and de-activate modification

of policies (i.e., .. **access profiles**))..

8.   As to claim 5, Graham teaches a **access control system where the**

access control system is implemented at least in part in the form of

software (i.e., ... teaches a system in accordance with the present invention

consists of server software running as an application on a standard hardware

configuration and client software either hooking into or running as a process on

top of the operating system on a standard hardware configuration [par. 31[).

9.   As to claim 6, Graham teaches a **access control system where the**

access control system is implemented at least in part in the form of

hardware (i.e., ... teaches a system in accordance with the present invention

consists of server software running as an application on a standard hardware

configuration and client software either hooking into or running as a process on

top of the operating system on a standard hardware configuration [par. 31[).

10.   As to claim 7, Graham teaches a **access control system where the**

access control system is arranged to govern user access profiles used by

a security device configured to control access to a data storage medium

(i.e., … teaches a proxy system interfaces with and maintains authentication, access and usage control and security across computer network utilization of content sources [par. 70]).

11.   As to claim 8, Graham teaches a **access control system where the security device is implemented at least in part in hardware and is of a type located between a data storage medium of a computing system and a CPU of the computing system** (i.e., …teaches DCMS client application being stored in the host Operating System's memory partition in the client computer [par. 397] Those skilled in the art would recognize a CPU is inherent to the hardware structure of a computer).

12.   As to claim 9, Graham teaches a **access control system where the security device is implemented at least in part in hardware and is of a type incorporated into bus bridge circuitry of a computing system** [fig. 14].

13.   As to claim 10, Graham teaches a **access control system where the access control system is incorporated into a computing system having an operating system and the current access profile is modifiable after loading of the operating system** (i.e., .. teaches includes a user interface, configured to facilitate creation and editing of said access policies and said usage policies and association of said access policies and said usage policies with said files [claim 6]).

14.   As to claim 11, Graham teaches a **method of controlling access to data**

stored on at least one data storage medium of a computing system, the

method comprising the steps of:

providing means for authenticating users permitted to access data

stored in the at least one data storage medium (i.e., … teaches user

authentication is performed by an authentication system and policy management

is accomplished by a policy system [par. 20]);

and storing data access profiles (i.e., … teaches access control

policies over managed content, such as files stored in a content source [par. 69]);

associating each data access profile one data storage medium (i.e.,

… teaches evaluates the user/file specific policy from the METAFILES and

database [par. 101]);

each data access profile including information indicative of the

degree of access permitted by a user to data stored in the at least one data

storage medium (i.e., .. teaches security on both an access and usage level

[par. 58]);

and each data access profile including a master data access profile

and a current data access profile and facilitating modification of the current

data access profile being within parameters defined by the master data

access profile (i.e., … teaches On a file creation, the METAFILE will

automatically inherit the policies of the parent directory [par. 206] … teaches

evaluates the user/file specific policy from the METAFILES and database [par.

101]);

15.   As to claim 12, Graham teaches a **method further comprising the step**

of facilitating creation of the master and current access profiles (i.e., …

teaches the authentication service creates credentials used to gain access to the

protected content [par. 105]).

16.   As to claim 13, Graham teaches a **method where the access control**

system is incorporated into a computing system having an operating

system (i.e., … teaches a server-side software modules uses many of the

standard functionality of commercial operating systems to accomplish its normal

operations [par. 72]), **and the step of facilitating modification of the current**

data access profile includes the step of facilitating modification of the

master data access profile only prior to loading of the operating system

(i.e., … teaches ervice performs internal policy consistency validation, rights

revocation, and synchronized policy updates [par. 111] Those skilled in the art

would recognize inherent to the boot process of computer is the updating of all

files] … further teaches at the time that the DCMS server application is booted, a

specified file path is checked. If there are Plug-Ins available, then the DCMS

server application loads these plug-ins, and continues booting [par. 371]).

17.   As to claim 14, Graham teaches a **method further including the steps**

of facilitating activation of said control system so as to permit modification

of the current access profile and facilitating deactivation of said control

system so as to prevent modification of the current access profile (i.e., ...

teaches a service performs internal policy consistency validation, rights

revocation, and synchronized policy updates [par. 111] Those skilled in the art

would recognize inherent to the capability to synchronize policy updates is the

ability to activate and de-activate modification of policies (i.e., .. **access**

profiles)).

18.   As to claim 15, Graham teaches a **method where the access control**

system is implemented at least in part in the form of software (i.e., ...

teaches a system in accordance with the present invention consists of server

software running as an application on a standard hardware configuration and

client software either hooking into or running as a process on top of the operating

system on a standard hardware configuration [par. 31[).

19.   As to claim 16, Graham teaches a **method where the access control**

system is implemented at least in part in the form of hardware (i.e., ...

teaches a system in accordance with the present invention consists of server

software running as an application on a standard hardware configuration and

client software either hooking into or running as a process on top of the operating

system on a standard hardware configuration [par. 31[).

20.   As to claim 17, Graham teaches a **method further comprising the step**

of arranging the access control system so as to govern user access

profiles used by a security device configured to control access to a data

storage medium (i.e., ... teaches a proxy system interfaces with and maintains

authentication, access and usage control and security across computer network

utilization of content sources [par. 70]).

21.   As to claim 18, Graham teaches a **method where the security device**

(i.e., DCMS) is implemented at least in part in hardware and is of a type

located between a data storage medium of a computing system and a CPU

of the computing system (i.e., ...teaches DCMS client application being stored

in the host Operating System's memory partition in the client computer [par. 397]

Those skilled in the art would recognize a CPU is inherent to the hardware

structure of a computer).

22.   As to claim 19, Graham teaches a **method where the security device is**

implemented at least in part in hardware and is of a type incorporated into

bus bridge circuitry of a computing system [fig. 14].

23.   As to claim 20, Graham teaches a **method further comprising the steps**

of incorporating the access control system into a computing system

having an operating system and facilitating modification of the current

access profile after loading of the operating system (i.e., ... teaches ncludes

a user interface, configured to facilitate creation and editing of said access

policies and said usage policies and association of said access policies and said

usage policies with said files [claim 6]).

24.   As to claim 21, Graham teaches a **computer program which when**

loaded into a computing system causes the computing system to operate

in accordance with an access control system for controlling access to data

stored on at least one data storage medium of a computing system, the

access control system comprising:

       authentication means to authenticate users permitted to access data

stored in the at least one data storage medium (i.e., ... teaches a content

subsystem regulates access to files in the content repository through the

evaluation and enforcement of authentication and access control policies [par.

85]);

       and database means (i.e., cache) **arranged to store data access**

profiles (i.e., ...teaches user shared session secrets and credentials are stored

in temporary caches [par. 98]);

       each data access profile being associated with a user permitted to

access data stored in the at least one data storage medium (i.e., ... teaches

the authentication service creates credentials used to gain access to the

protected content [par. 105]);

each data access profile including information indicative of the

degree of access permitted by a user to data stored in the at least one data

storage medium (i.e., ...teaches policies also state the restrictions to be placed

on content if access is granted. ... teaches enforced by the client module access

restrictions further define the operations permitted by the user on received

content [par. 173]);

and each data access profile including a master data access profile

and a current data access profile and the current data access profile being

modifiable within parameters defined by the master data access profile.

(i.e., ... teaches On a file creation, the METAFILE will automatically inherit the

policies of the parent directory [par. 206] ... teaches evaluates the user/file

specific policy from the METAFILES and database [par. 101]),

25.   As to claim 22, Graham teaches a **computer useable medium having a**

computer readable program code embodied therein for causing a computer

to operate in accordance with an access control system for controlling

access to data stored on at least one data storage medium of a computing

system, the access control system comprising:

authentication means to authenticate users permitted to access data

stored in the at least one data storage medium (i.e., ... teaches this

authentication interface obtains the identity or rights proving credentials used to

infer access rights [par. 127])

and database means arranged to store data access profiles (e.g., ...

authentication services) (i.e., ... teaches Entity information used by

authentication services is stored in the entity database [par. 114]);

each data access profile being associated with a user permitted to

access data stored in the at least one data storage medium (i.e., ... teaches

the authentication service creates credentials used to gain access to the

protected content [par. 105]);

each data access profile including information indicative of the

degree of access (i.e., condtype) permitted by a user to data stored in the at

least one data storage medium (i.e., ... teaches accConds Access Conditions

(multi-valued) 564 - the access conditions state the conditions under which

access will be allowed. Each condition consists of condType [par. 173; table 2]);

and each data access profile including a master data access profile

and a current data access profile, the current data access profile being

modifiable within parameters defined by the master data access profile (i.e.,

... teaches On a file creation, the METAFILE will automatically inherit the policies

of the parent directory [par. 206] ... teaches evaluates the user/file specific

policy from the METAFILES and database [par. 101]),

Contact Information

Any inquiry concerning this communication or earlier communications from

the examiner should be directed to BRYAN WRIGHT whose telephone number is

(571)270-3826. The examiner can normally be reached on 8:30 am - 5:30 pm

Monday -Friday.

If attempts to reach the examiner by telephone are unsuccessful, the

examiner's supervisor, AYAZ Sheikh can be reached on (571)272-3795. The fax

phone number for the organization where this application or proceeding is

assigned is 571-273-8300.

Information regarding the status of an application may be obtained from

the Patent Application Information Retrieval (PAIR) system. Status information

for published applications may be obtained from either Private PAIR or Public

PAIR. Status information for unpublished applications is available through

Private PAIR only. For more information about the PAIR system, see http://pair-

direct.uspto.gov. Should you have questions on access to the Private PAIR

system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-

free). If you would like assistance from a USPTO Customer Service

Representative or access to the automated information system, call 800-786-

9199 (IN USA OR CANADA) or 571-272-1000.

/BRYAN WRIGHT/
Examiner, Art Unit 2131
                              /Ayaz R. Sheikh/
                    Supervisory Patent Examiner, Art Unit 2131